UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF WISCONSIN

SEALED

UNITED STATES OF AMERICA

V.

CRIMINAL COMPLAINT

PHILIP H. WENTZEL(xx/xx/1971)

CASE NUMBER: 12-M-442

I, Jason Pleming, the undersigned complainant, being duly sworn, state the following is true and correct to the best of my knowledge and belief, in the State and Eastern District of Wisconsin, **Philip H. Wentzel**, the defendant herein engaged in the following conduct:

Count 1: In or about April of 2011, knowingly produced child pornography, in violation of Title 18, United States Code, Section 2251(a).

I further state that I am a Special Agent with the Federal Bureau of Investigation, and this complaint is based on the following facts:

Please see the attached affidavit of Special Agent Jason Pleming.

Continued on the attached sheet and made a part hereof: X Yes ___ No

Signature of Complainant
Jason Pleming

Sworn to before me and subscribed in my presence,

May 2nd 2012 at Milwaukee, Wisconsin
Date City and State

The Honorable William E. Callahan, Jr.
United States Magistrate Judge
Name & Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Jason Pleming, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation, and have been since September 2006. I am currently assigned to the Milwaukee Division Cyber Crimes Task Force (CCTF). As a Federal Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

2. This affidavit is being submitted in support of an Application for a Search Warrant for the residence located 9131 W. Cleveland Avenue (upper) West Allis, Milwaukee County, Wisconsin (hereinafter, "PREMISE-1"), and a 2009 Open Range 5th Wheel Recreational Vehicle, VIN 5XMFR332895000203, at campsite lot D25, [redacted] Campground, [redacted] State Road 67, Campbellsport, Fond du Lac County, Wisconsin, (hereinafter, "PREMISE-2"), in the State and Eastern District of Wisconsin, for evidence of violations of Title 18, United States Code § 2251(a), production of child pornography and Title 18, United States Code § 2252A, entitled "Certain activities relating to material constituting or containing child pornography."

3. Based upon the information summarized in this affidavit, I have reason to believe that evidence of such violations may be present at the residence located at PREMISE-1 and at PREMISE-2.

4. The information supplied in this affidavit is based upon my investigation and information provided and investigation conducted by other law enforcement personnel in this matter to date. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not set forth every fact related to or otherwise the product of this investigation.

DEFINITION OF TECHNICAL TERMS

5. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to an Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

d. Globally Unique Identifier (GUID): A GUID is a special type of identifier used in software applications to provide a unique reference number.

e. Peer-to-Peer Network (P2P): A P2P network allows users to trade digital files through a worldwide network formed by linking computers together via special software. Typically, users perform a keyword search to locate files, and the files can then be downloaded from any users in possession of those files. Users cannot send or receive files without consent.

PROBABLE CAUSE

6. On July 25, 2011, the Denver Division of the FBI executed a search warrant at a subject's residence who was alleged to be producing child pornography. The subject (hereafter referred to as Subject1) was interviewed and subsequently admitted to possessing, distributing and producing child pornography. Digital evidence was seized from Subject1's residence and transferred to the FBI for forensic analysis.

7. On August 10, 2011, a forensic review of Subject1's MacBook Pro laptop computer revealed a USB device named "FreeAgent GoFlex" had been disconnected from the MacBook Pro laptop at approximately 2:10 am on July 25, 2011. The original search warrant had been executed at approximately 12:45 pm that same day and this

device was not located during that search.

8. Based on this information, on August 12, 2011, a second search warrant was executed at Subject1's residence. The "FreeAgent GoFlex" 1TB hard drive was located hidden in the bed platform in the master bedroom. This hard drive was later found to be encrypted with TrueCrypt encryption and could not be accessed.

9. In late February 2012, Subject1 accepted a tentative plea agreement for full cooperation in exchange for a reduced prison sentence. Subject1 thereafter provided the password to his encrypted hard drive. Based on previous information developed during the investigation by the Denver FBI office, as well as the information from Subject1's hard drive and Subject1's subsequent debriefing, three additional subjects, all producers and hands-on offenders with multiple victims, were identified and later arrested in San Diego, CA; Kansas City, MO; and Pittsburgh, PA.

10. During a review of Subject1's hard drive, a folder was located called "Peps," which, according to Subject1, is where Subject1 stored all of the originally produced child pornography images and videos from other producers. One of the subfolders within the "Peps" folder was for an individual called [redacted] The [redacted] folder included two subfolders: [redacted] in addition to various other unsorted child pornography images. Per Subject1's debriefing, based on BitWise and Yahoo chats Subject1 had with [redacted] the girls to whom [redacted] claimed to have access were his nieces. [redacted] utilized the screen name [redacted] on BitWise and [redacted] on Yahoo. Subject1 confirmed that [redacted] and

[redacted] were the same individual.

11. Within the [redacted] folder, the majority of the child pornography images appear to have been taken while this unknown prepubescent girl was sleeping. In one such image, "HPIM5539.jpg," the unknown girl appears to be sleeping and an unknown male's erect penis is partially in the girl's mouth. In addition to the child pornography images of the girl, possibly named [redacted] there are two pictures of the same unknown girl standing outside in front of a fire pit. In one of the outside [redacted] images, your affiant observed several Recreational Vehicles (RV) parked at what appears to be an RV campground. The majority of the images of [redacted] were taken on April 21, 2011, based on the exif /metadata information affiliated with these images.

12. One of the outdoor [redacted] images where the unknown girl is standing outside in front of a fire pit was found to have been taken with a Samsung cell phone camera, Model SPH-M900, per the exif/metadata. Based on the exif/metadata of this image, GPS information was captured at the time the photo was taken. The GPS information is as follows: 43 40' 48" North latitude by 88 10' 31" West longitude. These coordinates were found to be in the vicinity of State Road 67, near [redacted] Campground, in Fond du Lac County, Wisconsin. The remaining images, the majority of which are of child pornography, were taken with a Hewlett-Packard (HP) PhotoSmart R927 camera, per exif/metadata. The other dates for the images in the [redacted] folder, taken with the HP camera, are May 28, 2010, and August 14, 2010.

13. In addition, found within the [redacted] folder, but not within the [redacted]

subfolder, are seven additional images which have almost identical GPS coordinates as the [redacted] images: 43 40' 48" North latitude by 88 10' 30" West longitude (the last coordinate is 30 instead of 31). These additional images were taken with the same Samsung SPH-M900 model cell phone camera, which took the outdoor photo of the girl believed to be [redacted] These images, per the exif/metadata, were taken on July 20, 2010, and July 21, 2010, and are of two unknown prepubescent girls sleeping on a sofa. Again, in these images, the girls appear to have been sleeping and/or drugged when the child pornography images were taken. One such image is of an unknown, prepubescent girl sleeping on a sofa, "2010-07-2101.46.44.jpg;" a male's hand has pulled down the girl's pajamas and underwear to expose the girl's vagina.

14. On March 7, 2012, FBI SA Tina Fourkas, Denver Division, located the user [redacted] on a Peer-to-Peer (P2P) file sharing program known to be utilized by individuals who trade child pornography. This user's profile was set up on October 27, 2011, and was last connected on December 20, 2011. The description on this user's profile page states: "If you know me from IMGSRC [redacted] my p/w here is the same as it is there. Otherwise, you show me yours, I'll show you mine. Girls only. 1-15: sleepers, hidden, selfshot, webcam, pee, diaper, panties(dirty), H/C dad/dau. Original work only. No web stuff. English only. Thanks."

15. On the same date, SA Fourkas located user [redacted] on imgsrc.ru, a Russian file sharing site. The "real name" of this user was listed as [redacted] The registered date for this user was listed as August 11, 2011. The user info stated: "Back

yet again. Keep comments clean I guess. Getting tired of bannings. English only. Girls I have to share range from 6-14. I work only now on 'you show me yours, I'll show you mine' basis. Don't blindly comment looking for passes unless you have same, hot little diaper girls, girls this age on cam or naughty girl self pics to share. No generic web stuff. If anything in your albums takes me to 'URL Cash' I do NOT respond. English only, please and thanks." This user was sharing seven different photo albums, four of which were password protected. The other albums had numerous pictures of clothed girls, many of which appeared to be the same girls or pictures from the [redacted] folder on Subject1's decrypted hard drive. To date, your affiant has been unable to locate IP connection logs for "[redacted]" since the website is hosted outside of the United States.

16. On March 19, 2012, this information, relative to [redacted] and the child pornography images with GPS coordinates, was provided to the Milwaukee office of the FBI.

17. On April 16, 2012, the GPS coordinates, referenced in paragraphs 13 and 14 above, were confirmed by FBI SA Richard Bilson to be located on the property of the [redacted] Campground in Campbellsport, Wisconsin. The outdoor area from the image of the unknown girl in front of the fire pit was then compared with GPS coordinates from the image. The image was found to be an exact match to Campsite Lot D-25 at [redacted] Campground.

18. On the same date, the owner of [redacted] Campground, [redacted] was

interviewed by FBI SA Lee Chartier and your affiant. [redacted] reported that Philip Wentzel (hereafter referred to as Wentzel) has leased lot D-25 since 2008. [redacted] advised that Wentzel first brought a trailer to lot D-25 in 2008, but then switched to a newer trailer in 2009. [redacted] stated that the new trailer has been permanently located on lot D-25 since 2009. [redacted] advised she regularly observes Wentzel present at the campground on lot D-25 on weekends during the camping season, which begins in approximately mid-April until mid-October.

19. [redacted] was shown non-pornography images of the two unknown prepubescent girls sleeping on a sofa referenced in Paragraph 14. [redacted] identified the girls as [redacted] and [redacted] (hereafter referred to as [redacted] and [redacted] respectively). [redacted] could identify the subjects as the [redacted] sisters but stated it was difficult to identify each one specifically since they both look very similar. [redacted] stated the first time she met the girls she thought they were twins. [redacted] was then shown the picture of the unknown girl standing outside in front of a fire pit, referenced in Paragraph 12. [redacted] identified the girl depicted in the image as [redacted] (hereafter referred to as [redacted], at a younger age. [redacted] related that [redacted] Wentzel. [redacted] advised that [redacted] has brought [redacted] to the campground in previous seasons.

20. [redacted] advised that [redacted] and [redacted] (hereafter referred to as [redacted], has leased lot [redacted] since 2010. [redacted] has never seen [redacted] wife at the resort, but stated during his divorce [redacted] was living in his

trailer at the campground, lot [redacted] and would ask [redacted] to check in on his children at night and make them dinner, because he was working [redacted] also recalled times when [redacted] was at the campground that [redacted] would watch the children, specifically [redacted] and [redacted] while [redacted] was working. [redacted] stated she interacted with [redacted] on several of these occasions as [redacted] would bring [redacted] and [redacted] into the campground's office and barn area to get pizzas. [redacted] knows [redacted] has asked other campers at the resort to look in on [redacted] and [redacted] Some of those same campers expressed concerns to [redacted] about the girls being left alone.

21. After completing the interview, [redacted] drove SA Chartier and your affiant to Wentzel's lot, D-25. I and SA Chartier observed an Open Range brand 5th wheel trailer located on lot D-25, which was the same location where the GPS coordinates were confirmed in Paragraph 18.

22. On April 25, 2012, I conducted a query of Wisconsin Department of Transportation records for all trailers registered to Wentzel. One of the trailers registered to Wentzel is a 2009 Open Range 5th wheel trailer.

23. On April 30, 2012, United States Postal Inspector Mark Spellman informed your affiant that Philip Wentzel receives mail at PREMISE-1. Further, SA Bilson and Cyber Crimes Task Force (CCTF) Officer Ungerer conducted physical surveillance on this date. The investigators observed a Black Chevrolet Silverado truck with Wisconsin registration plate DH1461 in the parking lot adjacent to PREMISE-1. A database check

of the license plate revealed that this truck is registered to Philip Wentzel.

24. I conducted an analysis of the [redacted] Yahoo! Account and observed that IP address 184.233.12.158 resolved back to Sprint PCS and was assigned to this account on April 21, 2011, at 05:01:55 (GMT) . An administrative subpoena request was sent to Sprint PCS on April 2, 2012. The subpoena results were received on April 10, 2012, and indicated that IP address 184.233.12.158 at 05:01:55 (GMT) was assigned to Philip Wentzel, [redacted] The subscriber history for Wentzel's account listed [redacted] as an account telephone number.

25. On April 27, 2012, I queried the Wisconsin Circuit Court Access website utilizing Wentzel's identifiers. The website reported that on January 6, 2012, Milwaukee County Court, Case No: 2012FA000144, received a divorce petition regarding the marriage of Wentzel and his wife, Dory Wentzel.

26. On April 4, 2012, I conducted a public records search. I searched the records utilizing Wentzel's identifiers. The search revealed that Wentzel's current address, as of March 2012, was [redacted]

27. Based on the information obtained via the [redacted] account and the information obtained through the Wisconsin Circuit Court Access website, I believe that Wentzel once lived at the Franklin, Wisconsin residence, referenced in the aforementioned paragraph; however, due to the divorce filing on January 6, 2012, I believe Wentzel is currently residing in the West Allis, Wisconsin residence.

28. On April 11, 2012, further information was received from Sprint regarding the

make and model of the cellular telephone associated with Wentzel's account. Sprint advised that the cellular telephone associated with this account is a Samsung M900 Slider SNG. Further, Sprint reported this cellular phone has been active on this account since November 2, 2009; however, Sprint related that in January 2012 said telephone number was ported out to another carrier. Therefore, Sprint is no longer providing service for this account as it relates to said telephone number.

29. On April 26, 2012, I conducted an Internet query for "Samsung M900 Slider SNG". One of the Internet results directed your affiant to Samsung's website, which displayed a Samsung cellular telephone with the model number of SPH-M900. Based on this result and the Sprint records, I believe the cellular telephone assigned to Wentzel is the same make and model of the cellular telephone that took the pictures referenced in Paragraph 12 and 14.

30. An analysis of the Yahoo account [redacted] IP logs revealed two instances where this account was accessed via 204.194.251.5, which resolved to "Milwaukee County Government" on the dates 8/1/2011 07:33:31 and 8/2/2011 09:45:13 (GMT). The analysis also revealed numerous instances where this account was accessed via IP address 65.30.60.220 and IP address 67.52.13.238 between October 26, 2011 and November 27, 2011.

31. On April 4, 2012, administrative subpoena results were received from Time Warner/Road Runner in reference to IP addresses 65.30.60.220 and 67.52.13.238 used by [redacted] IP address 65.30.60.220 listed the user as [redacted]

[redacted] West Allis, WI (Wentzel's current address) and IP address 67.52.13.238 listed to the Community Justice Resource Center, 906 W. Historic Mitchell St., Milwaukee, WI 53204.

32. On April 12, 2012, confidential source (hereafter referred to as CS1) provided IP connection logs for [redacted] Between December 13, 2011, and December 20, 2011, [redacted] was seen logging into their account from IP address 67.52.13.238 and 65.30.60.220.

33. On April 30, 2012 administrative subpoena results were received from Time Warner / Road Runner for IP addresses 67.52.13.238 and 65.30.60.220 for the dates listed in the aforementioned paragraph. Time Warner reported that IP address 65.30.60.220 listed to [redacted] West Allis, WI (Wentzel's current address). In addition, Time Warner reported that IP address 67.52.13.238 listed to the Community Justice Resource Center, 906 W. Historic Mitchell St., Milwaukee, WI 53204.

34. On April 3, 2012, a review of [redacted] Facebook page revealed the following: [redacted] lists [redacted] as her school [redacted] in Milwaukee, Wisconsin); [redacted] lists [redacted] as her current home town; [redacted] lists her favorite teacher [redacted]; one of [redacted] friends on Facebook is [redacted].

35. On April 9, 2012, [redacted] was interviewed by FBI SA Brett Banner and CCTF Officer Brant Ungerer. [redacted] advised she is a Title One Teacher for the City of Milwaukee, specifically assisting [redacted]

[redacted] was shown the same images of the minor females that were shown to [redacted] specifically, the non-pornography images of the two unknown prepubescent girls sleeping on a sofa referenced in Paragraph 14. [redacted] stated she could not be certain but thought that the individual in the images looked like [redacted] also stated that [redacted] has a sister, [redacted], which looked similar to her, but that [redacted] was shorter. [redacted] could not identify the individual depicted in the picture of the unknown girl standing outside in front of a fire pit, referenced in Paragraph 12.

36. [redacted] has taught the [redacted] sisters for the past three years, instructing them in reading and math. [redacted] instructs the students one hour each day on Tuesdays and Thursdays. The students are taught in small groups at the [redacted] commented that the sisters behave well in her class but that [redacted] time with each child is only two hours each week. [redacted] is aware that the [redacted] parents are divorced and that the children are "bounced" between homes. [redacted] commented that [redacted] has mentioned several times that [redacted] considers [redacted] to be her favorite teacher and that [redacted] also wishes [redacted] was her mother. The girls have also mentioned to [redacted] that they go camping [redacted] during the summer.

37. [redacted] has noticed that [redacted] has become quiet this year and that [redacted] has missed a lot of school this year. Two years ago, [redacted] recalled that [redacted] had finger mark bruises on her arm. [redacted] expressed concern for the childrens' welfare.

38. In April, 2012, I conducted a Google search on Wentzel. This search revealed several Milwaukee newspapers articles in which Wentzel, in his official capacity as a law enforcement officer with the Milwaukee County Sheriff's Department, is quoted concerning Milwaukee County Sheriff's Department matters. I believe that Wentzel is a Milwaukee County Sheriff Deputy. I also believe Wentzel has utilized several online accounts and identities ([redacted] and [redacted] to trade child pornography images and videos. From the IP connections logs obtained during this investigation, Wentzel has utilized these accounts at several locations to include his residence in West Allis, Wisconsin and his possible place of employment in Milwaukee, Wisconsin.

39. Based upon my training and experience, I know that individuals involved in the distribution of child pornography routinely utilize P2P file sharing programs to distribute images and videos of child pornography. As stated in Paragraph 16, SA Fourkas located user "[redacted] on imgsrc.ru. On said site this user listed his "real name" as "[redacted]. I believe that "[redacted] is the same user who has utilized the Yahoo account of "[redacted] and P2P account "[redacted] I believe this based on the fact that, in his online profile, "[redacted] also lists himself as [redacted]. Moreover, the same IP address (65.30.60.220) was used to login in to the "[redacted] account and the "[redacted] account. On both instances, Time Warner reported that said IP address listed to the address of PREMISE-1 (Wentzel's current residence). I further believe that since "[redacted] identified himself as

[redacted] (which is an account known to have advertised child pornography) in his P2P account, that it is probable he utilized the [redacted] account to distribute child pornography from IP 65.30.60.220.

40. As referenced above in Paragraph 10, additional subjects have been identified in this investigation by the Denver office of the FBI. Specifically, the subject located in Pittsburgh, PA (hereafter referred to as Subject2) was arrested on February 15, 2012, for allegedly producing child pornography. On March 26, 2012, Subject2 was interviewed by FBI agents from the Pittsburgh office of the FBI. Subject2 advised that he had utilized the following tools to access and/or distribute child pornography: Bitwise, Yahoo Messenger, and imgsrc.ru. Regarding the use [redacted] Subject2 stated he thought [redacted] lived in Wisconsin and had been taking pictures of two young girls he had adopted. Subject2 recalled that [redacted] worked "midnight shift" somewhere in Wisconsin. Subject2 advised seeing images of young girls where [redacted] was penetrating the girls with his fingers. In addition, Subject2 related that sometimes [redacted] would send Subject2 cash to give to minor females (Subject2 had groomed two minor females to regularly perform sex acts for him) so that [redacted] could watch Subject2 perform live sex acts on the minor females via the Internet.

41. Denver SA Fourkas provided your affiant with a copy of the evidence found within Subject1's hard drive referenced in Paragraph 11. I reviewed the images found within the [redacted] folder" and observed numerous images of child pornography

to include child pornography images of an unknown male spreading apart the vagina of a prepubescent female and attempting to digitally penetrate her.

42. Based on my training and experience, I know that users of P2P file sharing programs, like the one used by [redacted], generally store the electronic files that they are sharing on their computers or on other electronic storage devices. Based on my training and experience, I also know that these computers and storage devices are generally kept at the user's residence.

43. Further, I believe Wentzel utilized his Sprint Cellular telephone, Samsung M900, to produce child pornography and then traded those child pornography files with Denver's defendant, Subject1. Based on the GPS data contained within the child pornography images and my observations while at the [redacted] campground, I believe Wentzel produced the child pornography images while inside his Open Range 5th wheel trailer located on Lot D-25.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

44. This application seeks permission to search for records that might be found on the PREMISE-1 and PREMISE-2, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

45. Probable cause. I submit that if a computer or storage medium is found at

PREMISE-1 or PREMISE-2, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or

delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

46. Forensic evidence. This application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer at PREMISES1 or PREMISES2 because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of

its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

47. Necessity of seizing or copying entire computers or storage media. In most cases, a thorough search of the premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information.

Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

48. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard

drive to human inspection in order to determine whether it is evidence described by the warrant.

49. Because more than one person shares PREMISE-1 as a residence, it is possible that the PREMISE-1 will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

Statement of Probable Cause in Support of Application

50. Based on the facts as I have stated them in this affidavit, there is probable cause to believe that evidence of violations of Sections 2251 and 2252A of Title 18 of the United States Code is located at PREMISE-1 and PREMISE-2. "Attachment A" to this affidavit is a list of items that would be the subjects of search and seizure at these locations.

51. The locations, PREMISE-1 and PREMISE-2 are more particularly described as follows:

PREMISE-1 is a two story building that encompasses two businesses on the lower level and [redacted]

PREMISE-2 is an Open Range brand 5th wheel light grey colored trailer with a grey colored "swoosh" design on its sides. The trailer is mounted onto a structure that is covered with lattice and located on lot D-25. A mulch garden is located at the front of the trailer and a green colored storage shed with brown doors is located behind the trailer. A deck with white decorative fencing surrounding the deck is adjacent to the trailer. In addition, a wooden picnic area is permanently built into the hillside adjacent to the deck.